Garbage-man-in-the-middle attack on the LUC4 cryptosystem.

Abstract

This paper reports an investigation into an attack on the LUC4 cryptosystem. LUC4 cryptosystem is derived from a fourth order linear recurrence relation and is based on the Lucas function. This cryptosystem is analogous to the RSA, LUC and LUC3 cryptosystems. Therefore, the security for this cryptosystem is similar to the RSA cryptosystem because they are depend on the intractability of factorization. There are numerous mathematical attacks on RSA-type cryptosystem, one of them is polynomial attacks. The garbage-man-in-the-middle attack is one of the polynomial attacks on LUC4 cryptosystem. This type of attacks is exploiting the polynomial structure of RSA. Based on the analysis and implementations, the security aspects will be looked into and appear to depend on the intractability of factorization.

Keyword: LUC4 cryptosystem; Public key cryptography; RSA cryptosystem.